Procedure No. 2205.06: Use of E-mail and Instant Messaging
Reference: POLICY NO. 2206
Effective: 12/28/04
Prior Issue: 04/30/04

Purpose:

The Arizona Department of Juvenile Corrections (ADJC) establishes rules for all computer users within ADJC.

Rules:

1. **MANAGEMENT INFORMATION SERVICES (MIS) PERSONNEL** shall provide Internal Department E-mail with each user account unless specifically denied by the user's supervisor.

2. **USERS DESIRING INTERNET E-MAIL, GROUPWISE MESSAGING, AND WEB E-MAIL ACCESS** shall complete an application, Form 2206.01A, and turn it in to their supervisor.

3. If the supervisor approves the application, the **SUPERVISOR** shall send the application to the MIS Chief Information Officer (CIO) or designee who shall install the requested service.

4. **USERS** shall be aware of the following:
   a. Both the nature of e-mail and the public character of the Department's business make e-mail less private than users may anticipate. For example, e-mail intended for one person sometimes may be widely distributed because of the ease with which recipients can forward it to others. Even after a user deletes an e-mail record from a computer or e-mail account it may persist in whole or in part in system logs, in the directories of the person who received the message, or on system back-up tapes which may be retained for long periods of time. All these items may be subject to disclosure under applicable law and this policy and procedure. The MIS Department cannot routinely protect users against such eventualities;
   b. E-mail, regardless of whether created, received, or stored on Department equipment, may constitute an "Official Record" (as defined by A.R.S. § 41-1350); may be a "Public Record" subject to disclosure under the Arizona Public Records Law (A.R.S. § 39-121); or may also be subject to disclosure or access under other laws or as a result of litigation;
   c. The Department does not automatically comply with all requests for disclosure, but attempts to evaluate such requests against the precise provisions of the Public Records Law or other applicable law concerning disclosure and privacy;
   d. The Department, in general, cannot and does not wish to be the arbiter of the contents of e-mail and Instant Messaging. Employees are strongly urged to use the same personal and professional courtesies and considerations in e-mail as they would in other forms of communication and particularly those applicable to written communications since e-mail creates a tangible record of that communication;
   e. Inappropriate e-mail use may expose the Department and individual users to claims for damages through copyright infringement, libel, breach of privacy or other personal or proprietary rights. No e-mail rule-based forwarding outside of ADJC's domain is permitted. If rule-based forwarding needs to be done, it needs to be encrypted;
   f. Federal law and Department policies regarding copyright and intellectual property apply to e-mail. Do not violate the copyright of others. Unless the material is legally established as being in the public domain or there is an explicit release from the copyright owner, you may not copy e-mail information. Under the copyright law, you may or may not have a copyright on e-mail material that you create. Check with the appropriate authority before assuming that you have a copyright on such material;
   g. Instant Messaging services can be provided through Department systems. The Department does not allow Instant Messaging systems outside of the Department network.

5. **USERS** may not access, use, or disclose personal or confidential information without appropriate authorization, and shall take necessary precautions to protect confidentiality of personal or confidential information, regardless of whether the information is maintained on paper or is found in e-mail or other electronic records.

6. **USERS** shall follow sound professional practices in providing for the security of e-mail records, archives, and proxy access under their jurisdiction:
   a. **USERS USING A COMMON OR GROUP COMPUTERS** shall close their personal e-mail account after using GroupWise;
   b. **USERS** shall not email any attachment larger than 10,240k (10 Megabytes) internal or external to the Agency:
      i. **USERS** shall contact MIS to facilitate the transferring of attachments larger than 10 megabytes to recipients;
      ii. **MIS** shall guard against such large emails from transversing the network using network policies to enforce.

7. **USERS** shall guard against storage media deterioration and e-mail record inaccessibility due to hardware or software becoming obsolete. To eliminate these situations, **USERS** shall make provision for future accessibility by:
   a. Transferring all official e-mail records to the next generation of hardware or software;
   b. Transferring only current official e-mail records to new hardware or software; or
   c. Converting official e-mail records not transferred to other media "eye readable form" for long term storage and preservation.

8. **USERS** shall safe guard their identification codes and passwords and use them only as authorized:
   a. **USERS** are responsible for all e-mail transactions made under the authorization of their identification, and for all network e-mail activity originating from his or her computer;
   b. **USERS** shall not use e-mail identifications for commercial purposes;
   c. **USERS** shall not loan or sell access to user identifications.

9. E-mail Proxy access is the sole responsibility of the Employee. The **OWNER OF AN E-MAIL ACCOUNT** may grant rights to access their e-mail to other employees. By default, proxy access is disabled for everyone.

10. **ANY USER** shall report any virus or malicious code infections within e-mail to MIS.

11. The **DEPARTMENT** may permit the inspection, monitoring, or disclosure of e-mail when:
   a. Required by or consistent with applicable law or policy such as Arizona Public Records law (A.R.S. § 39-121, regarding inspection of public records); the Family Educational Rights and Privacy Act or any appropriately issued subpoena or court order. The Electronic Communications Privacy Act of 1986 also permits messages stored on Department systems to be accessed by authorized personnel in certain circumstances;
   b. There is a reasonable suspicion that violations of law or Department policy have occurred or may occur; or
   c. There are time-dependent, critical operational needs in connection with Department business and the Department determines that the information is not readily available through other means.

12. In such instances, the **DEPARTMENT** shall, as a courtesy, normally try to inform e-mail users prior to any inspection, monitoring, or disclosure of e-mail records, except when such notification would be detrimental to an investigation of possible violation of law or Department policy or procedure.

13. **USERS** are required to comply with Department requests for access to and copies of e-mail records when access or disclosure is required or allowed by applicable law or policy, regardless whether such records reside on a computer housed or owned by the Department. Failure to comply with such requests can lead to disciplinary or other legal action pursuant to applicable law or policy/procedure, including but not limited to appropriate Department policies and procedures.

14. The confidentiality of electronic messaging systems cannot be assured, and any confidentiality may be compromised by access consistent with applicable law or policy, including this Policy, by unintended redistribution, or due to current technologies inadequate to protect against unauthorized access. **USERS,** therefore, shall exercise extreme caution when communicating confidential or sensitive matters, and should not assume that their electronic conversation is private or confidential.

15. **USERS** shall not use e-mail for illegal activities. Illegal use may include, but is not limited to:
    a. Obscenity;
    b. Child pornography;
    c. Threats;
    d. Harassment;
    e. Theft;
    f. Attempting unauthorized access to data or attempting to breach any security measures on any electronic communications system;
    g. Attempting to intercept any electronic communication transmissions without proper authority;
    h. Violation of copyright, trademark or defamation law.

16. In addition to illegal activities, **USERS** shall not engage in the following e-mail practices:
    a. Entering, examining, using, transferring, and tampering with the accounts and files of others, unless appropriately authorized pursuant to this procedure;
    b. Altering e-mail system software or hardware configurations; or
    c. Interfering with the work of others or other computing facilities.

17. **USERS** shall follow state law with regard to the disposition of e-mail records. Failure to do so may lead to criminal charges. Theft or unauthorized destruction, mutilation, defacement, alteration, falsification, removal or secretion of e-mail records may lead to class 4 or class 6 felony charges under A.R.S. § 38-421.

18. If a user has been requested by another user via e-mail or in writing to refrain from sending e-mail messages, the **USER WHO RECEIVES SUCH A REQUEST** shall not send that user any further e-mail messages until such time as s/he has been notified by the system administrator that such correspondence is permissible. Failure to honor such a request shall be deemed a violation of this procedure.

19. **USERS** shall not use Department e-mail services for:
    a. Commercial activities not approved by appropriate supervisory Department personnel;
    b. Personal financial gain;
    c. Uses that violate other Department policies or guidelines:
        i. Applicable Department policies. These include, but are not limited to, policies and guidelines regarding personnel, intellectual property, or regarding sexual or other forms of harassment.
    d. Uses inconsistent with applicable state or federal law.

20. **USERS** shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the Department or any unit of the Department unless expressly authorized to do so. Where appropriate, the user shall include the following explicit disclaimer: “The opinions or statements expressed herein are my own and should not be

taken as a position, opinion, or endorsement of the Arizona Department of Juvenile Corrections."

21. **USERS** shall not use Department electronic messaging services for purposes that could reasonably be expected to cause, directly, or indirectly, strain on any computing facilities, or cause interference with anyone's use of electronic messaging systems. Such uses include, but are not limited to, the use of electronic messaging services to:
    a. Send or forward chain letters;
    b. "Spam" systems for the purposes of widespread distribution of unsolicited mail;
    c. Non work-related "Letter-bomb," that is, to resend the same e-mail repeatedly to one or more recipients;
    d. Express opinions of your own through unsolicited e-mail. This may or may not include, but is not limited to, political and religious opinions; and
    e. Sexual or other forms of harassment.
    f. Use of unsolicited email originating from within ADJC's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the agency or connected via ADJC's network.
    g. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

22. **USERS** shall confidentially report suspected or known violations of policy, procedure, or law to the appropriate supervisory level for the operational unit in which the violation occurs. Violations shall be processed by the appropriate authorities and/or law enforcement agencies. Violations may result in revocation of e-mail service privileges; disciplinary action up to and including dismissal; referral to law enforcement agencies; or other appropriate legal action.

23. **MIS** shall be responsible for safeguarding the Department network and critically sensitive information from e-mail contaminants per State of Arizona Government Information Technology Agency (GITA) Policy P800-S860: MIS shall:
    a. Protect all workstations and servers with virus-scanning software that has a "notify and clean," a function that will prevent users from changing the above information as stated in Policy 2205.03;
    b. Scan all incoming e-mail including attachments for the existence of virus or malicious codes;
    c. Scan all incoming e-mail for open relay servers and block such e-mail from reaching its intended recipient. (An open relay is an e-mail server that allows third-party relaying of e-mail messages where the sender cannot be verified);
    d. Scan for prohibited and/or offensive words and phrases that are commonly used in spamming, chain letters, etc.

Effective Date:	Approved by Process Owner:	Review Date:	Reviewed By: